An Overview of Distributed Computing in the Cloud and BlockChain for Safeguarding the Healthcare Sector

Jhansi Bharathi Madavarapu[1*], Shailaja Salagrama[2], Jami Venkata Suman[3],
Subba Rao Polamuri[4], K.Reddy Madhavi[5,] Shiva Kaleru[6]

[1, 2]Department of Information Technology, University of the Cumberland's,
Williamsburg, Kentucky, USA
*jhansimadavarapu@gmail.com
shailajasalagramass@gmail.com
[3]Department of ECE, GMR Institute of Technology, Rajam, India
venkatasuman.j@gmrit.edu.in
[4]Department of CSE, BVC Engineering College, Odalarevu, India
psr.subbu546@gmail.com
[5]Department of AI&ML, School of Computing, Mohan Babu University.
kreddymadhavi@gmail.com
[6]Juniper Networks, USA
shivakaleru@gmail.com

Abstract. The need for patient-centered electronic records that can store and retrieve the myriad details of a patient's medical history as documented during treatment has increased dramatically. These records are vital for future care, billing, or treatment. The distributed ledger technology known as Blockchain enables us to store this data and start and enable use at lightning speed while keeping the system transparent and secure. Using a distributed system with ledger capability allows for the safe and interoperable storage of records. With the elimination of mediators in financial and data transactions and in verifying data authenticity and ownership records, blockchain technology promises to alter the current state of digital asset transactions radically. Its extensive files and easy access to patients' medical histories are two of the most critical issues in healthcare, and its immutability, decentralization, and openness make it an ideal solution. Interoperability, the ability of various health organizations and software product makers to connect and exchange data securely and smoothly, is crucial to healthcare systems' practical and successful operation. Lack of interoperability is the root cause of many difficulties in contemporary healthcare, including data silos and disparate workflow tools. To solve this problem, a system that allows safe, recognized medical records to be kept in separate databases should be implemented. Using fog computing, which can decentralize data processing and handle massive amounts of data, we reviewed the literature and performed a system overview of blockchain technology in this study. Our ongoing experimental study highlights areas where current systems are lacking and suggests potential avenues for further research.

Keywords: Block Chain, Healthcare System, Fog Computing

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_134

1. Introduction

To run their businesses efficiently, modern healthcare providers want real-time data access and are open to embracing innovative technologies. Businesses engage in a broad range of transactions daily, such as processing orders and making payments to each other, to maintain the flow of commerce. The time wasted waiting for verification from unbiased third parties and the possibility of human mistake is increased because each user must record their transactions in their ledger. That is why it is essential to have a shared ledger; that way, everyone involved in the transactions will see the same accurate record. As its name suggests, a blockchain system records all transactions in an immutable ledger known as a "block," formed whenever a new transaction is executed. This ledger is publicly available. Everyone may trust the digital proof recorded in the distributed ledger since an impartial third party is no longer needed to validate transactions. Distributed ledgers record and verify all transactions, similar to an audit trail, so everyone involved in the healthcare system (hospitals, doctors, pharmacies, labs, etc.) can use the data as-is or make any required changes. The use of permission-based access control rules to protect sensitive data necessitates stringent privacy restrictions that differ for each agent's role.

Blockchain technology is secure and decentralized because it relies on a shared ledger that only authorized users (such as the company's suppliers or agents) can access. Once all participating agents have validated a transaction, it is considered finalized. Once confirmed, no user in the system can erase it.

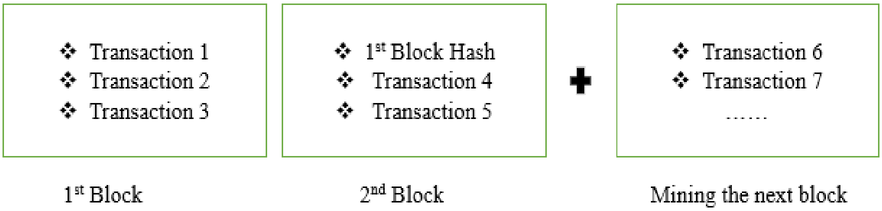

Fig. 1. Blockchain

To better understand blockchain technology, it can be helpful to picture it as an impenetrable, encrypted database that stores sensitive patient information. Blockchain technology allows for the trading of digital assets. It works by creating users who agree on the terms of the transactions and validate them at regular intervals. The consensus is recorded in the distributed ledgers. The timestamping technique that defines the distributed ledger adds the timestamped records of transactions to an ever-expanding list. This is what makes up a blockchain. Each block's hash or fingerprint value is connected to the previous one to build a decentralized database. A decentralized ledger records atomic transactions and verifies their key attributes directly, cutting out middlemen. You can use that Blockchain to confirm the current status of whether the previous block's hash was included in the next block's hash. The most important things are the date and the guarantee that a specific transaction occurred. This work can be utilized as "proof of work" to maintain and expand the Blockchain. They can safeguard their sensitive data with a permanent identity, and the evidence will be helpful for verification. The system is accessible to all program users because of the underlying computer network.

While blockchain data is unchangeable, privacy problems arise due to the public nature of the ledger. Carefully documenting who has access to what portions of a patient's health information is crucial. Simply said, Blockchain was never intended to store an enormous amount of data. Including a decentralized storage solution in healthcare theory could greatly alleviate the Blockchain's absence of a universal reference standard. Due to the lack of a central point of failure or data loss, blockchain networks offer greater flexibility than centralized ones. Fog computing is revolutionizing the way data, services, and resources are typically distributed by moving the emphasis from the central cloud to the network's edge nodes. The Fog network design uses more than just network admission to bring structure and efficiency to the otherwise disorganized Internet.

One way to think about the infrastructure supporting cloud computing is a complex network of interconnected computer systems, with individual server nodes serving as the building blocks for higher-level connections. Users get fast access to the data since the fog nodes store and process it locally. The phrase "perimeter computation" appears frequently in fog computing. Getting one's functional and cognitive capacities close to the information source is crucial for navigating through the fog and the peripheral. Remember that these designs rely on the same physical resources for data transmission. No matter if they are electrical circuits or sensors, all of these systems contribute to the actual world in some way. This decentralized security is achieved through the usage of blockchain technology. This study shows how Blockchain could be useful in various environmental data processing.

2. Literature Survey

According to "Zhao, Huawei, et al.," a medical blockchain's key management system is highly efficient [1]. Blockchain technology has nearly universal support as a potential game-changer in the healthcare industry. Before healthcare limits gain momentum, the blockade discussion must resolve the issue of health data privacy. This study's authors address the unique requirements of health blockchains by developing a biosensor network that can quickly and easily restore critical blockchain data from a lightweight backup.

Mr. Sandro Amofaetal. Data Exchange of Individual Health Records using a Blockchain Foundation for Security. With the help of a community-developed acceptable use policy and blockchain-based smart contracts, health information exchanges can safely handle individual data. As established by accredited medical facilities, hospital policy dictates the permissible and prohibited uses of patients' medical records. You can get these rules from the system and use them to determine if data can be transferred via smart contracts. Secure computation and access to patient data are achieved by the combined efforts of processing nodes, smart contracts, and security monitors from participating healthcare facilities.

The third, The "ACP" Approach to Blockchain-Powered Parallel Healthcare Systems, was proposed by Wang, Shuai, et al. For PHSs, developers have created an artificial system framework for parallel execution ("ACP"). The Healthcare Community Blockchain Consortium's goal, built on the most recent version of blockchain technology, is to bring administrative agencies, patients, and healthcare providers together. A place where medical records may be reviewed and shared and oversight processes can be audited.

This study employs cloud computing to build a system for safely transferring individual health records based on Blockchain. "Zheng, Xiaochen, and colleagues." The potential application of blockchain and cloud storage for the safe and transparent transfer of individuals' real-time, dynamic health data was covered in [4]. A Customized Approach to the Exchange of Health Records Users can securely and confidentially exchange their medical records using blockchain technology and the cloud.

Xia, Qi et al.'s "A system that tackles the problem of medical data sharing across medical big data custodians in a trust-less environment" states as much [5]. Using the Ethereum blockchain, MeDShare ensures that patients' personal information remains private while it is transferred between different cloud providers. Big data organizations can benefit from this method by using distributed ledger technology to build a centralized database for all their shared medical records and then control who has access to it. In addition to all system operations, an immutable log records all data transfers and exchanges within MeDShare. The article explains how to quickly revoke access data in case of a violation by monitoring data series behavior in real time.

"The System Timing analysis for inferring the topology of the Bitcoin peer-to-peer network," published by "Neudecker, Till, et al." in [6], offers proof that timing data may be used to infer network topology. A method for timing analysis that shows promise in theory and practice for preventing flooding in peer-to-peer networks. In a real-world Bit currency network where such attacks could happen, we will use recognition to show that notification cooperative networks can handle essential accuracy and memory. Method for determining the flooding network topology by measuring the flooding duration.

In a newly published article titled "Fog Computing as a Defensive Approach

Against Distributed Denial of Service (DDoS)," the authors offer a strategy for shielding networks from DDoS assaults. To safeguard clouds from distributed denial of service (DDoS) attacks, Paharia, Bhumika, et al. [7] proposed an additional design layer called Filter Fog. This article proposes a device that can enhance the standard building design method. One way of looking at cloud computing is as an attempt to strengthen the security of data stored in the cloud. Cloud infrastructure increasingly uses fog computing to defend against distributed denial of service (DDoS) attacks and other ever-changing threats. This paper outlines a plan to prevent distributed denial-of-service attacks from accessing the cloud using fog computing.

In their citation, Naidu, Vishal, and others assert that [8] Full-Transparency Supply Chain Management is Built on Blockchain and the Internet of Things. From the origin of the raw materials to the point of sale, decentralizing this information might lead to a more flexible and transparent system. Once turned on, this feature will speed up data flow across the system compared to a traditional centralized supply chain management method. Utilizing This should lead to a reduction in the system's mistake rate. Efficiency gains will improve customer service across the board in the supply chain. Spot face supply inconsistencies at different supply chain nodes, reproduced and followed.

Method for Zhao, Huawei, and colleagues [9] The health services industry stands to gain much from the Blockchain above regarding app pricing. The growing trend of individuals keeping large amounts of sensitive medical records secret is an issue that needs fixing. Before their broad use, health blockchains must resolve their security problems. A network of sensors is being placed throughout the human body to provide minimal backups and essential efficient recovery strategies for health deterrents. Body sensor networks (BSNs) are a new technological innovation that can potentially improve people's health.

As per the publication by Chen, Zhonglin, et al. titled "A Security Authentication Scheme of 5G Ultra-Dense Network based on Blockchain" [10], the authors of the paper go over a method of "5G UDN" security authentication that is enabled by blockchain technology. This paper presents APG-PBFT, a new algorithm integrating Blockchain and the PBFT consensus method. The main problem that the "Mobile Security Authentication Scheme" for "UC" access to "UCE." tries to solve is how to build trustworthy access points, similar to APG.

3. System Overview

To avoid needing a "Trusted Third Party," experts advise that researchers create and deploy a fog computing system for healthcare data that stores all records on a single blockchain. As a result of the system's efforts, end users' data is now secure, private, and inconsistent.

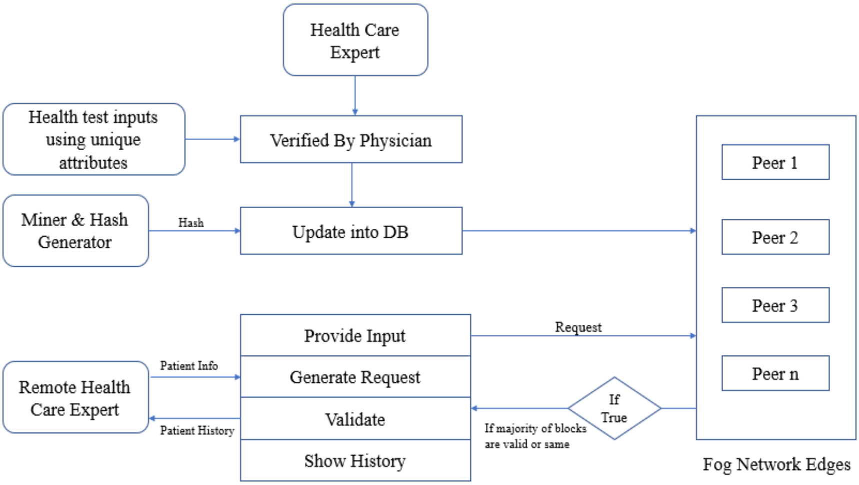

Fig. 2. System Overview

The use of blockchain technology to store medical records is notable in the system. With the help of fog networks, a patient's entire medical record can be accessible to a new doctor in another city if they are recommended there; blockchain technology will guarantee the data's security at all times.

The associated transactions are processed across multiple servers utilizing a sequencing fog network because of the massive amounts of data. The issue with time limits and service quality is now better understood. This middleware system's processing environment uses threads to offer load balancing. An identical copy of the newly created request will exist on every node in the Blockchain [11]. We will employ a hashing algorithm to generate a hash from your supply text. We use peer-to-peer verification to ensure the information is accurate before completing any transaction [12]. The current server blockchain will be restored or updated if any chains become damaged. The query will not be committed until all nodes have been checked. A mining algorithm is used to verify that the hash that is generated for the query is valid.

4. Conclusion

Discovering the safest way to implement Blockchain technology in a real-world context requires substantial technical research. Additional investigation into developing secure and economically viable Blockchain packages is necessary before it is used to drive a redistribution application. For example, "via performance metrics associated with time and value of computations or assessment metrics associated with its feasibility" might be used to compare and contrast Blockchain-based health care concepts with existing systems. Alternatively, academics are considering enhancing the capabilities of existing Blockchains or creating a Blockchain specifically for the healthcare business, as new Blockchain networks are occasionally superior to the ones currently in place. Research on applying the proposed system with multiple data nodes will be intriguing. Very few proposed solutions to the privacy and security problems with Blockchain have been tested or even studied. Blockchain also has two unexplored scaling concerns: throughput and latency.

References

1. Zhao, H.: Efficient key management scheme or health blockchain. CAAI Transactions on Intelligence Technology 3, 114-118 (2018)
2. Amofa, S.: A Blockchain-based Architecture Framework for Secure Sharing Personal Health Data. In IEEE: 20th International Conference on e-Health Networking, Applications and Services, pp. 1-6. IEEE Press, Ostrava, Czech Republic (2018)
3. Wang, S.: Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. IEEE Transactions on Computational SocialSystems 99, 1-9 (2018)
4. Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J.: Blockchain-based Personal Health Data Sharing System Using Cloud Storage. In IEEE: 20th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-6. IEEE Press, Ostrava, Czech Republic (2018)
5. Xia, Q.: MeDShare: Trust-less medical data sharing among cloud service providers via Blockchain. IEEE Access 5, 14757-14767 (2017)
6. Neudecker, T., Andelfinger, P., Hartenstein, H.: Timing Analysis for Inferring the Topology of the Bitcoin Peer-to-Peer Network. In IEEE: International Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, pp. 358-367. IEEE Press, Toulouse, France, (2016)
7. Paharia, B., Bhushan, K.: Fog Computing as a Defensive Approach Against Distributed Denial of Service (DDoS): A Proposed Architecture. İn IEEE: 9th International Conference on Computing, Communication and Networking Technologies (ICT), pp. 1-7. IEEE Press, Bengaluru, India (2018)
8. Naidu, V., Mudliar, K., Naik, A., Bhavathankar, P.: A Fully Observable Supply Chain Management System using Block Chain and IOT. In IEEE: 3rd International Conference for Convergence in Technology (I2CT), pp. 1-4. IEEE Press, Pune, India (2018)
9. Zhao, H., Zhang, Y., Peng, Y., Xu, R.: Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys. In IEEE: 13th International Symposium on Autonomous Decentralized System (ISADS), pp. 229-234. IEEE Press, Bangkok, Thailand (2017)
10. Chen, Z.: AsecurityAuthentication Scheme of 5G Ultra-Dense Network Based on Block Chain. IEEEAccess 6, 55372-55379 (2018)

11. Madavarapu, J.B., Yalamanchili, R.K., Mandhala, V.N.: An Ensemble Data Security on Cloud Healthcare Systems: 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), pp. 680-686, Trichy, India (2023)
12. Kshetri, N., Jeffrey, V.: Blockchain-Enabled E-Voting. IEEE Software 35, 95-99 (2018)